Hybrid C-SCRM Policy and Governance Lead (Intelligence Analyst)

Who We Are

C2I was established in 2018 and comprises high-trust, high performance colleagues and friends from the military, government, and private industry. We bring the right people, technology, and data to help clients predict and mitigate traditional and evolving risks in sensitive government and commercial activities. We generally team with like-minded firms to deliver extraordinary technology and services to our clients. Together we help government and commercial clients illuminate risk, streamline decision-making, and achieve mission success. We are seeking a Hybrid Cyber Supply Chain Risk Management (CSCRM) Governance Lead. This position will focus on developing policies and procedures to structure a SCRM program intended to mitigate risks associated with the agency's supply chain and third-party vendors. This role involves creating and maintaining a comprehensive cyber risk management framework, ensuring compliance with security standards and regulatory requirements, and overseeing governance processes to protect the organization’s assets and data. They will also work to develop and incorporate contract and acquisition policies with associated terms and conditions to ensure all agreements align with the agency's security standards and risk management objectives.

What You Will Do

Develop Comprehensive Cyber Supply Chain Policies:

- Establish policies that define the security requirements and expectations for all supply chain partners and third-party vendors.
- Ensure policies cover key areas such as data protection, incident response, access controls, and secure software development.
- Align policies with industry standards (e.g., NIST SP 800-161) and regulatory requirements (e.g., GDPR, CCPA).

Policy Implementation and Enforcement:

- Develop procedures to enforce compliance with established policies.
- Implement monitoring mechanisms to ensure adherence to policies and procedures.
- Collaborate with internal teams to integrate policy requirements into procurement and vendor management processes.

Continuous Improvement and Policy Updates:

- Regularly review and update policies to address new threats and vulnerabilities.
- Gather feedback from stakeholders to improve policy effectiveness.
- Stay informed about industry best practices and regulatory changes to ensure policies remain current.

Risk Management Framework:

- Design and Maintain Risk Management Framework.
- Create a framework for identifying, assessing, and mitigating risks associated with the supply chain and third-party vendors.
- Implement risk assessment tools and methodologies to evaluate the security posture of vendors and suppliers.

- Develop risk mitigation strategies and action plans to address identified vulnerabilities.

Integrate Risk Management with Governance:

- Ensure the risk management framework is integrated with governance processes to provide oversight and accountability.
- Establish key risk indicators (KRIs) and key performance indicators (KPIs) to monitor the effectiveness of risk management activities.

Governance and Oversight:

- Establish Governance Committees.
- Form and lead governance committees or working groups focused on third-party risk management.
- Develop governance structures to ensure clear roles, responsibilities, and accountability.
- Develop and Maintain Risk Registers: Create and maintain third-party risk registers to document and track identified risks.

Monitor and Report on Governance Activities:

- Generate regular reports on the status of governance activities, including policy compliance and risk management efforts.
- Present findings and recommendations to senior leadership and relevant stakeholders.

Due Diligence and Onboarding:

- Conduct thorough due diligence on potential vendors and third-party partners.
- Ensure security requirements are integrated into vendor selection and onboarding. Collaborate with procurement and legal teams to negotiate contracts that include robust security clauses.

Contract and Acquisition Policy Integration:

- Develop and incorporate security and risk management requirements into contract and acquisition policies.
- Ensure all vendor agreements and contracts include terms and conditions that align with the company's security standards and risk management objectives.
- Review and update contract terms and conditions regularly to address evolving risks and regulatory requirements.

What We Are Looking For

15 years relevant experience with Bachelors in related field; 13 years relevant experience with Masters in related field; 10 years relevant experience with PhD or Juris Doctorate in related field; or High School Diploma or equivalent and 19 years relevant experience.

Bachelor's degree in Cybersecurity, Information Technology, Business Administration, or a related field.

Minimum of 10 years of experience in policy creation, governance, and risk management in supply chain or third-party risk management.

Strong knowledge of cybersecurity principles, risk management frameworks, and regulatory requirements (e.g., NIST, ISO 27001, GDPR).

Experience developing and implementing risk management policies and governance frameworks.

Proven experience in integrating security requirements into contract/acquisition policies and managing terms/conditions in vendor agreements.

Excellent analytical, problem-solving, and communication skills.

Ability to work independently and as part of a team in a fast-paced environment.

Possess and maintain a current TS-SCI clearance.

Preferred: Bonus Points For -

Familiarity with supply chain management and federal acquisition procurement processes.

Experience with governance, risk, and compliance (GRC) tools and software.

Knowledge of emerging threats and trends in cybersecurity and supply chain risk management.

Relevant certifications (CISSP, CISM, CRISC, or CTPRP, etc.)

Opportunity and Benefits

We are a Service-Disabled Veteran-Owned Small Business with seasoned veterans from the military, government, and private sector. C2I offers exciting work, competitive compensation, and opportunities for professional growth. Benefits include paid time off, medical, and life insurance. We are an equal opportunity employer committed to recruiting, training, and promoting qualified people of all backgrounds without regard to race, color, religion, sex, pregnancy, age, national origin, ancestry, citizenship status, sexual orientation, gender identity, marital status, uniformed services, veteran status, disability, genetic information, or any other protected characteristic as established by law.

Senior Governance Insider Threat Policy SME (Intelligence Analyst)

Who We Are

C2I was established in 2018 and comprises high-trust, high performance colleagues and friends from the military, government, and private industry. We bring the right people, technology, and data to help clients predict and mitigate traditional and evolving risks in sensitive government and commercial activities. We generally team with like-minded firms to deliver extraordinary technology and services to our clients. Together we help government and commercial clients illuminate risk, streamline decision-making, and achieve mission success. We seek a full-time Senior Governance Insider Threat (InT) Policy SME to support our customer in the Centers for Medicare and Medicaid Services (CMS) effort. This individual will work full-time hybrid, with on-site work in Woodlawn, Maryland, and may travel up to 10%. Potential to work up to 3 days on-site; and at least 2 days remotely. This CMS effort supports technology development, threat analysis, operations integration, training support, data analytics support, and technology transition assistance.

What You Will Do

- Serve as an Insider Threat Policy Subject Matter Expert, tasked with drafting, reviewing, and achieving finalized program status with documentation, policies, and procedures IAW applicable Federal Law, Executive Orders, Presidential Decision Directives, and local agency policy.
- Gather, analyze, evaluate, and prepare recommendations for program improvements, organizational process changes, optimization, development, and / or administration efforts for insider threat programs and analysis, network activity assessments, including user entity behavior analysis, and other security-related programs as assigned.
- Advise the customer on drafting complementary security, insider threat and intelligence-related policies, procedures, and handbooks to enable information sharing, analysis, and other InT activities in a non-Title 50 (Non-IC), non-Title 10 (Non-DoD) environment.
- Develop, draft, edit, and review policy, procedures, and processes to conduct an effective insider threat analysis and security program.
- Prepare, produce, edit, and disseminate formal and informal reports, summaries, and products as directed by [contractor and government] leadership.
- Provide advice, recommendations, and oversight to policy and procedure development relating to insider threat, security, and analysis.

What Eligible Candidates Must Possess

- 9 years relevant experience with Bachelors in related field; 7 years relevant experience with Masters in related field; or High School Diploma or equivalent and 13 years relevant experience.
- Experience drafting, reviewing, and editing documents, policies, and procedures concerning insider threat-related matters.
- US Citizenship required.
- Clearance: Must possess and maintain a Top Secret clearance with eligibility for Sensitive Compartmented Information (SCI), including willingness to take and pass a CI Scope Polygraph.
- Proficiency in using the Microsoft Office suite of programs, including Office 365.

Preferred: Bonus Points For -

- 10+ years' experience and familiarity with insider threat operations and analysis with a master's degree or bachelor's with 15+ years of InT experience.
- Experience conducting insider threat analysis and activities in a Title-50 or Title-10 environment.
- Experience conducting insider threat analysis and activities in a non-Title-50 or non-Title-10 environment.
- Graduate of a US Government Insider Threat course.
- Thoroughly familiar with National Insider Threat Task Force standards and EO 13587.

Opportunity and Benefits

We are a Service-Disabled Veteran-Owned Small Business with seasoned veterans from the military, government, and private sector. C2I offers exciting work, competitive compensation, and opportunity for professional growth. Benefits include paid time off, medical, and life insurance. We are an equal opportunity employer committed to recruiting, training, and promoting qualified people of all backgrounds without regard to race, color, religion, sex, pregnancy, age, national origin, ancestry, citizenship status, sexual orientation, gender identity, marital status, uniformed services, veteran status, disability, genetic information, or any other protected characteristic as established by law.